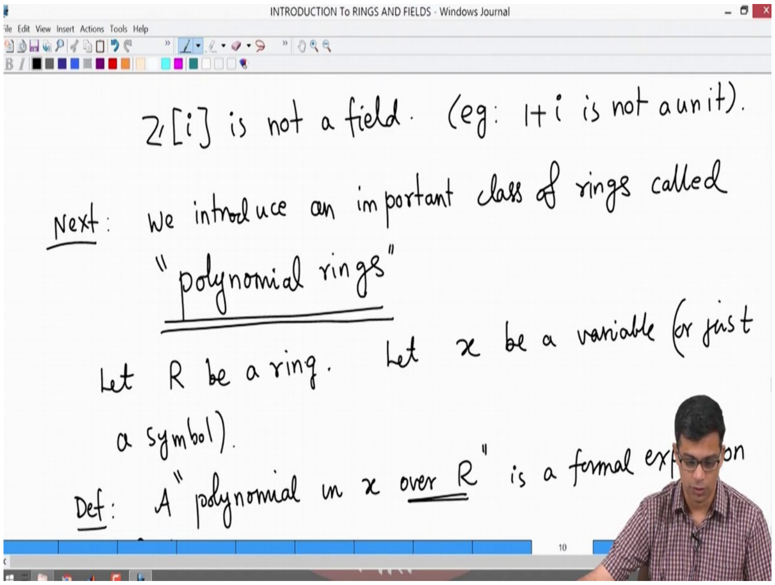
# Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

## Lecture - 04
## Polynomial rings 1

(Refer Slide Time: 00:17)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
10

$\mathbb{Z}[i]$ is not a field. (eg: $1+i$ is not a unit).

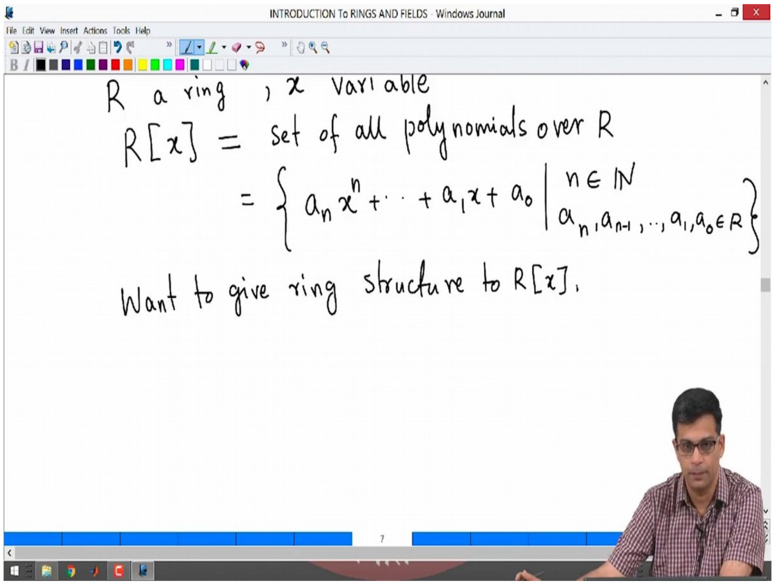
Next: We introduce an important class of rings called "polynomial rings"

Let $R$ be a ring. Let $x$ be a variable (or just a symbol).

Def: A "polynomial in $x$ over $R$" is a formal exp on

So, let us continue with the study of polynomial rings, in the last video I talked about what polynomials over a ring R are. So, let us quickly recall that, then today we will discuss that we make it a polynomial ring ok.

(Refer Slide Time: 00:40)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

R a ring , $x$ variable

$R[x]$ = set of all polynomials over R

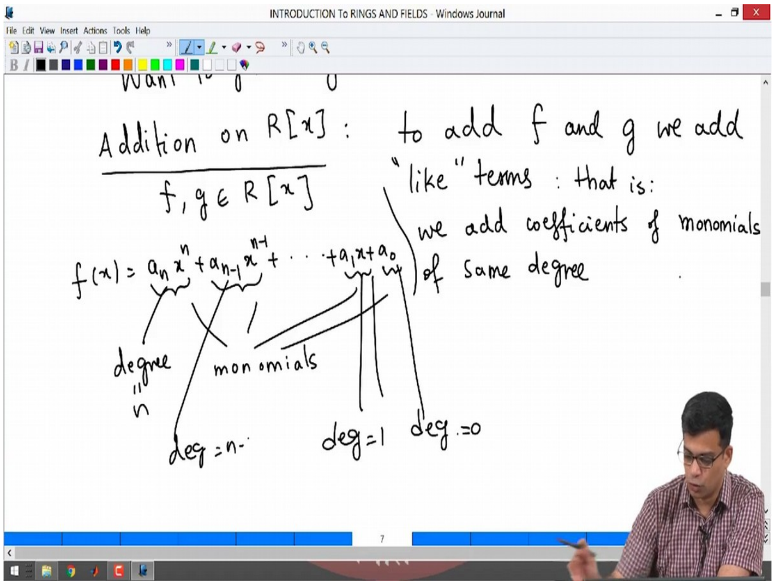
$$= \left\{ a_n x^n + \cdots + a_1 x + a_0 \;\middle|\; \begin{array}{l} n \in \mathbb{N} \\ a_n, a_{n-1}, \ldots, a_1, a_0 \in R \end{array} \right\}$$

Want to give ring structure to $R[x]$.

So, if R is a ring; R is any ring remember we used notation R square bracket x where x is a variable ok. So, remember I told you that variable means it is a just a symbol it has no meaning; so it is just a symbol. So, this is the set of all polynomials over R. So, I told you what those are these are expressions of the form. So, this is like this a n x n plus dot dot dot a 1 x plus a 0, where n is a natural number and a i's are all elements of the ring R. Remember that we can choose, we have to take all polynomials; that means, we have to take small n for every natural number and consider all polynomials with all the coefficients being any elements of the ring R.

So now, the next thing is we want to give a ring structure to R[x]. So, this is our next goal. What is a ring structure? Remember from the definition of a ring that we gave some time ago, a set is called a ring if it has two operations, we usually call them addition and multiplication. Under addition it has to an abelian group, multiplication has to satisfy some properties, but it need not have inverses and addition and multiplication  have to distribute. So, there is one natural way to add and multiply polynomials, so let us recall what that is.

(Refer Slide Time: 02:36)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

Addition on R[x] : to add f and g we add "like" terms : that is: we add coefficients of monomials of same degree

$f, g \in R[x]$

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

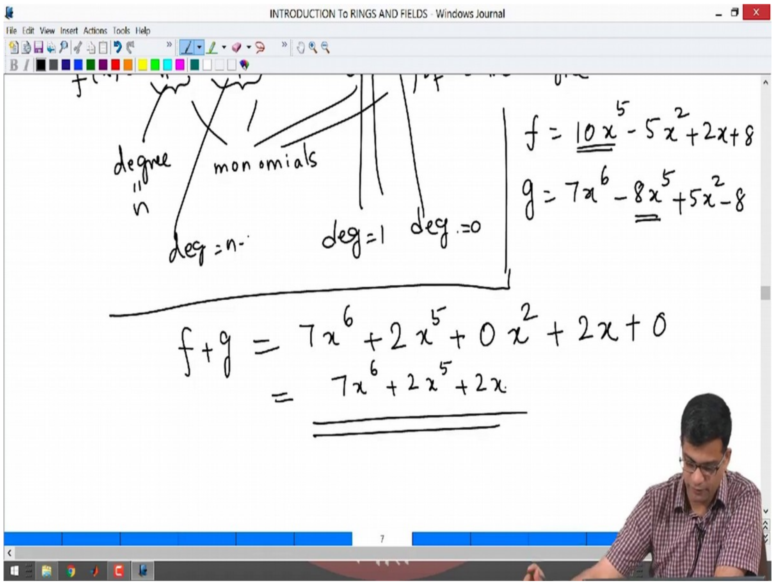
degree = n
monomials
deg = n-
deg = 1
deg = 0

So, to add polynomials, so in order to make R x ring we have to define addition on R x and multiplication on R x addition is the something that you can guess. So, take two polynomials; so basically to add I will write it like this first, to add two polynomials we simply add, let us say f and g are elements of the polynomial ring, in other words they are polynomials, to add f and g we add like terms ok. So, I will explain this, so we add like terms. So, what does this mean? So, when I say like terms that is, we add monomials, coefficients of monomials of same degree ok.

So, I do not know if I mentioned this, but if you have a polynomial something like a n x n plus an minus 1 x n minus 1 this is a polynomial meaning lot of terms, a single term of this is called a monomial. So, this is a monomial; this is a monomial; this is a monomial. So, these are all monomials. And what is the degree a monomial? Degree of a monomial is this degree is n, this degree is n minus 1, this degree is 1, this degree is 0 remember degree simply stands for the exponent of x.

So, each monomial has a degree to it and we add coefficient of monomials of same degree. So, in other words; so it is actually very easy to understand this. So, I will just give you one example to describe this.

(Refer Slide Time: 04:56)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
degree = n
monomials
deg = n-
deg = 1
deg. = 0

$f = \underline{\underline{10x}}^5 - 5x^2 + 2x + 8$

$g = 7x^6 - \underline{\underline{8}}x^5 + 5x^2 - 8$

$$f + g = 7x^6 + 2x^5 + 0x^2 + 2x + 0$$

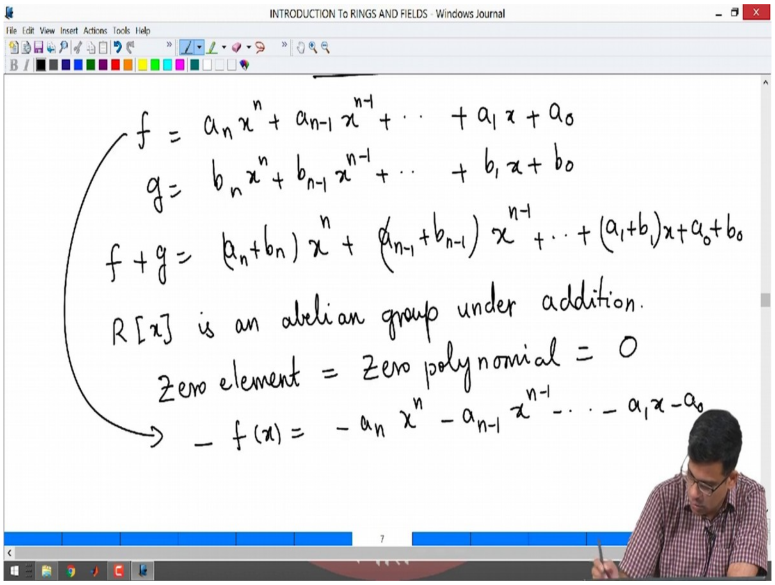
$$= \underline{\underline{7x^6 + 2x^5 + 2x}}$$

Let us say f is 10 x 5 minus 5 x square plus 2 x plus 8 ok. So, you can think of this as a polynomial with integer coefficients and let us say g is 7 x power 6 minus 8 x power 5 plus 5 x squared minus 8 ok. So, what would be f plus g? So, f plus g would be so, you remember you have to add like terms. So, you compare terms the largest degree that you have in x, in f is 5 largest degree you have in g is 6.

So, comparing order degree 6 monomial there is only 1, so that is 7 x power 6. Now, to add the next monomial x power 5 is common to both, so it will be 10 x 5 minus 8 x 5 so, this is 2 x 5 ok. So, this is the we add coefficients; we add the coefficients of like terms, so this is similar to this ok. So, 10 plus minus 8 is 2; so that is 2 x 5.

There are no other terms until x squared. So, x power 4 is not present in both x cubed is not present in both, but x square is present in both and the coefficients are minus 5 and 5, so this is just 0 x squared. So, I am writing it now, but we do not need to write it in general and now next we have to compare x terms, there is x in f no x in g, so that is a 2 x and we have 0. So, f plus g is actually just 7 x power 6 plus 2 x power 5 plus 2 x, so that is f plus g.

(Refer Slide Time: 06:57)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$g = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

$$f + g = (a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \cdots + (a_1 + b_1) x + a_0 + b_0$$

R[x] is an abelian group under addition.

Zero element = Zero polynomial = 0

$$- f(x) = - a_n x^n - a_{n-1} x^{n-1} - \cdots - a_1 x - a_0$$

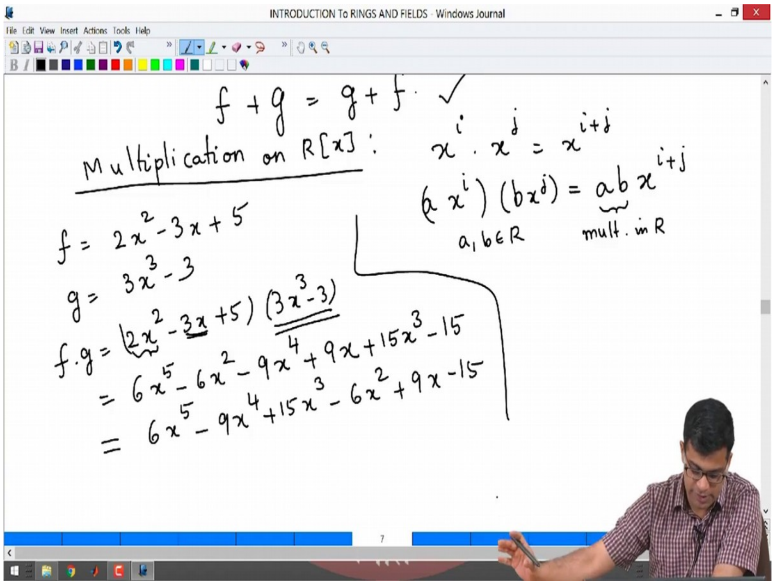
So, you understand how to add two polynomials, so you simply add like terms. So, we can formally write the definition as let us say f is a n x n, a n minus 1 x n minus 1 a 1 x plus a 0 g is let us say b m x n b n x n n b n minus 1 x n minus 1, b 1 x plus b 0 and in order to write the same n here I am allowing a n or b n to be 0. So, here of course, if I write like this f will be 0 times x power 6 first term; so a n and b n can be 0.

So, then f plus g 1 of them will be 0 may be not both of them of course, this will be a n plus b n x n, a n minus 1 plus b n minus 1 x n minus 1, so on, a 1 plus b 1 x plus a 0 plus b 0, ok. So, this is a very natural way to add polynomials. So, this is the addition and I will simply assert here that under addition R[x] is an abelian group under addition ok. This is very easy to check the coefficients are inside a ring; so, the coefficients are in a ring which is an abelian group under addition.

So, coefficients satisfy group properties and here to add two polynomials you are really not worrying about x; x is just like a place holder, x tells us what is the degree that is all and essentially we are adding elements of R. We are adding elements of R in various degrees because addition in R satisfies group axioms addition in R[x] also satisfies group axioms. What is the zero element? Is the zero polynomial right; so, the zero polynomial has all coefficients 0, that is a zero element. What is minus of f(x)? So, if f is like this if f is an x n plus a n minus 1 x n minus 1 and so on, what is minus of f, that is clearly just minus a n x n minus x n minus a n minus 1 x n minus 1 and so on minus a 1 x minus a 0.

And associativity certainly holds and you have a, in other words, a group, so, so far so good right. So, we are trying to give a ring structure to R[x], we have defined an addition and under that we see that it is an abelian group.

(Refer Slide Time: 10:01)



INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
7

$f + g = g + f. \checkmark$

Multiplication on R[x] :

$x^i \cdot x^j = x^{i+j}$

$(a x^i)(b x^j) = \underbrace{ab}_{\text{mult. in } R} x^{i+j}$

$a, b \in R$

$f = 2x^2 - 3x + 5$

$g = 3x^3 - 3$

$f.g = (2x^2 - 3x + 5)(3x^3 - 3)$

$= 6x^5 - 6x^2 - 9x^4 + 9x + 15x^3 - 15$

$= 6x^5 - 9x^4 + 15x^3 - 6x^2 + 9x - 15$

$= 6x^5 - 9x^4$

It is an abelian group right because f plus g is g plus f, that is because the addition of elements of R is communicative and adding elements in R[x] in other words adding polynomials is just adding elements of just like adding elements of R. So, this is ok; so its abelian group.

So, next what is multiplication? So, next we want to understand what is multiplication on R[x]. So, this is also very similar and we slightly more technical, but you have to get used to this, it is not difficult. So, we first learn how to multiply two monomials, so and that is natural. So, if you have x power i and x power j, how do you multiply them you simply take it to be x power i plus j; on the other hand if you have a x power i and b x power j; remember a and b are elements of the ring.

So, ax power i b x power j I will define it to be ab x power i plus j, remember a b is actually multiplication in the ring R. So, this is multiplication in R because a and b are in R, I can multiply them because R is the ring which has multiplication. So, this is multiplication in R and x power i terms x power j is x power i plus j.

Now, that we know how to multiply single monomials we can simply generalize this to define multiplication of any polynomials. So, I will write an example first and that will tell you how to multiply and then I will write the formal expression for multiplication, so again a very simple example. So, let us you have x f is 2 x square minus 3 x plus 5, I am just taking arbitrary polynomials and you have 3 x cubed minus 3 let us say ok.

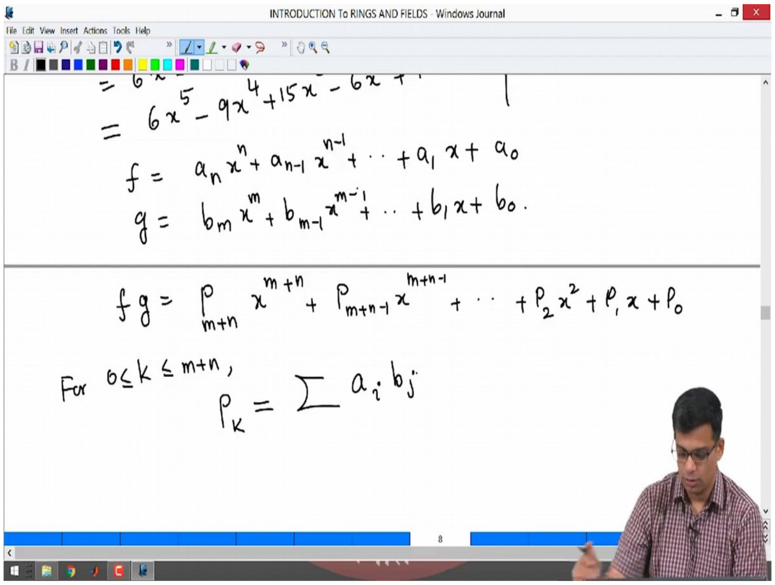
So, it is just like adding the way you add numbers in when you add two numbers and multiply with another number. So, how do you multiply f and g? So, what we have to do is 2 x cubed minus 3 x plus 5 times 3 x cubed minus 3. So, how do we multiply? So, I will first think of this 2 x cubed and multiply this polynomial. So, what is 2 x cubed times this polynomial I will multiply one monomial at a time. So, 2 x cubed times 2 x, so this is 2 x squared; 2 x squared times 3 x cubed is because of the rule that I wrote here it is 6 x power 5, next I will multiply this with minus 3, so I get minus 6 x squared. So, I have taken care of 2 x squared next I look at 3 x.

So, minus 3 x times 3 cubed, so that will give me minus 9 x to the 4th and then minus 3 x times minus 3 that will give me 9 x and finally, I have 5 times 3 x cubed. So, that is 15 x cubed and minus 5 times minus 3 is minus 15. So, now all you need to do is combine like terms. So, that for example, here are there any like terms actually there are no like terms here.

So, you can just put the degrees in the decreasing order. So, you get 6 x 5 minus 9 x 4, but in general if you have x squared may appear twice in which case you will just add the coefficients of x squared. So, in this case what we have is minus 9 x 4 plus 15 x cubed minus 6 x squared and plus 9 x minus 15. So, hopefully this gave you some idea of how to multiply polynomials ok.

So, all you need to do is repeatedly do this multiplication of single monomials, you have several monomials in the first polynomial, you have several monomials in the second polynomial and you can multiply a monomial at a time.

(Refer Slide Time: 14:22)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$= 6x$

$= 6x^5 - 9x^4 + 15x - 6x +$

$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

$g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0.$

$fg = P_{m+n} x^{m+n} + P_{m+n-1} x^{m+n-1} + \cdots + P_2 x^2 + P_1 x + P_0$

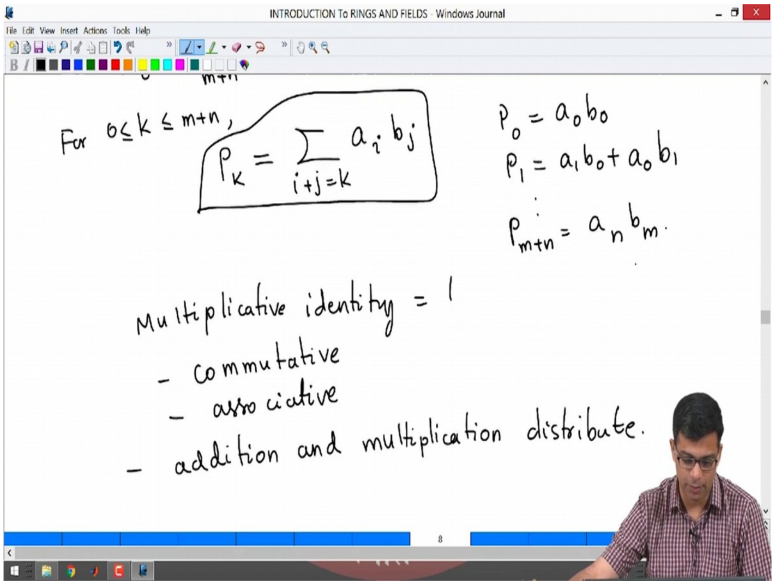
For $0 \leq k \leq m+n$,

$P_k = \sum a_i b_j$

So, what would be the general formula for multiplication? So, general formula; so for that let us write f as a 0 a n x n plus a n minus 1 x n minus 1, a 1 x plus a 0; g is b m x m b m minus 1 x m minus 1, all the way up to b 1 x plus b 0. So, let us say f times g, I want to describe f times g, what is this? So, f times g, I will first write the general so, the largest degree term will be mn, ok.

So, P mn x sorry this is m plus n because x n times x m is m n plus P m plus n minus 1 x m plus n 1 minus 1 all the way up to P 2 x squared P 1 x plus P 0. So, I am using P i's to denote the coefficient of f g. Now, I need to tell you how to find the coefficients P i, because in order to tell what f g is and it to simply tell you what are coefficients are this coefficients will be described in terms of the coefficients of f and g.

(Refer Slide Time: 15:49)



INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
8

$m+n$

For $0 \leq k \leq m+n$, $\boxed{P_k = \sum_{i+j=k} a_i b_j}$

$P_0 = a_0 b_0$

$P_1 = a_1 b_0 + a_0 b_1$

$\vdots$

$P_{m+n} = a_n b_m$.

Multiplicative identity $= 1$

- commutative
- associative
- addition and multiplication distribute.

So, what is P k? So, for any k; so let me write it like this for k between 1 or 0 and m plus n, P k is equal to ok. So, if I; I mean I will write down the formula you can quickly check using the example and the definition of multiplication of monomials that this is correct and this is fairly straight forward. In order to get x power k term in the product, we have several, we have how to get x power k term in the product, we can multiply two monomials in f one in; f one in g whose degrees add up to k there might be several such choices.

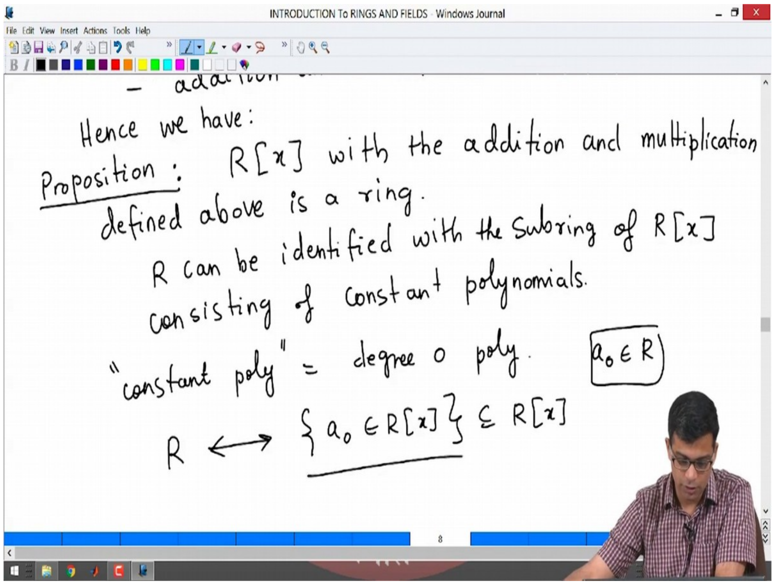
For example, to get x power 5 you can multiply x term in f x power 4 term in g, x squared term in f x cubed term in g, x cubed term in f x square term in g and so on. So, we have to add a i times b j, we have to multiply the coefficients of the corresponding terms for every i, j which add up to k right. So, this is the expression for coefficient of f g.

So, in particular we know P 0 will simply be a 0, b 0, which is not surprising right because to get the constant of f g, you must there is only one possibility you have to multiply the constant in terms of f and g. Similarly, what is P 1? To get the linear term, degree 1 term of f g you can multiply the linear term of f with constant term of g that will give me a 1 b 0. Similarly, I can multiply the constant term of f with linear term of g, so and so on. And finally, what is P m plus n? This is simply a m or a n b m ok. So, this tells me how to get all the coefficients of the product, and again I will simply assert these without proof which can be checked easily and these are not difficult and they are not very illuminating to check.

So, I will simply write that there is a multiplicative identity, simply 1. So, we denote multiplicative identity any way by 1 in any ring. So, 1 will continue to be multiplicative identity here because if you multiply any polynomial by the constant polynomial 1 you get 1.

And, multiplication is commutative right because, ok, this requires a little thinking, but ultimately because multiplication in the base ring R is commutative, multiplication in the polynomial for polynomials also is commutative; it is certainly associative, multiplication is associative and finally, addition and multiplication distribute, ok. This is also again ultimately because addition and multiplication distribute in the ring R, so they distribute in the set R[x] also.

(Refer Slide Time: 19:16)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
8

– addition

Hence we have:

Proposition: R[x] with the addition and multiplication defined above is a ring.

R can be identified with the Subring of R[x] consisting of constant polynomials.

"constant poly" = degree 0 poly. $\boxed{a_0 \in R}$

$R \longleftrightarrow \underline{\{a_0 \in R[x]\}} \subseteq R[x]$

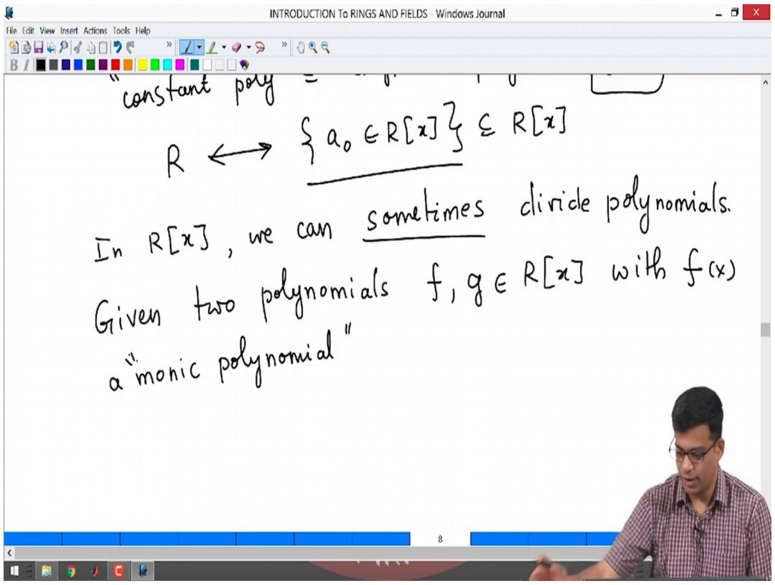
So, conclusion of all this is I will write this as a proposition; hence we have a proposition: R[x] with the addition and multiplication defined above is a ring ok. So, I have not proved this, I will not prove this; I will only write this and we will; obviously, use this a lot this is an important example of a ring for us.

So, this is an ring with the addition and multiplication defined above, we can add and multiply polynomials, so it becomes a ring it has all the required properties. And, more over R can be identified with this with the sub ring of R[x] consisting of constant polynomials. So, what are constant polynomials? Constant polynomials are polynomials of degree 0; so, constant polynomial is degree 0 polynomial ok. So, inside R x you have degree 0 polynomials. So, these are just, what is a degree 0 polynomial? So, it is just of the form a 0 right with a 0 in R.

So, R can be identified with the set of a 0 in R[x], this is a very obvious statement because you a constant polynomial has no x in it all the data that is required to describe a constant polynomial is just a 0. So, this is a sub ring of R[x] that one can check quickly because you can add elements and you will land here and you can multiply you land here one is there and so on. So, this is a sub bring and R can be identified with this.

So, this is important for us, we have constructed a new ring starting with a ring R, we have constructed a new ring and we called it the polynomial ring and the new ring contains R as a sub ring, so this is an important point. So, now let us study these polynomial rings a little bit more, I want to introduce an important concept here: we want to be able to divide polynomials.

(Refer Slide Time: 22:16)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

"constant poly" =

$R \longleftrightarrow \underline{\{ a_0 \in R[x] \}} \subseteq R[x]$

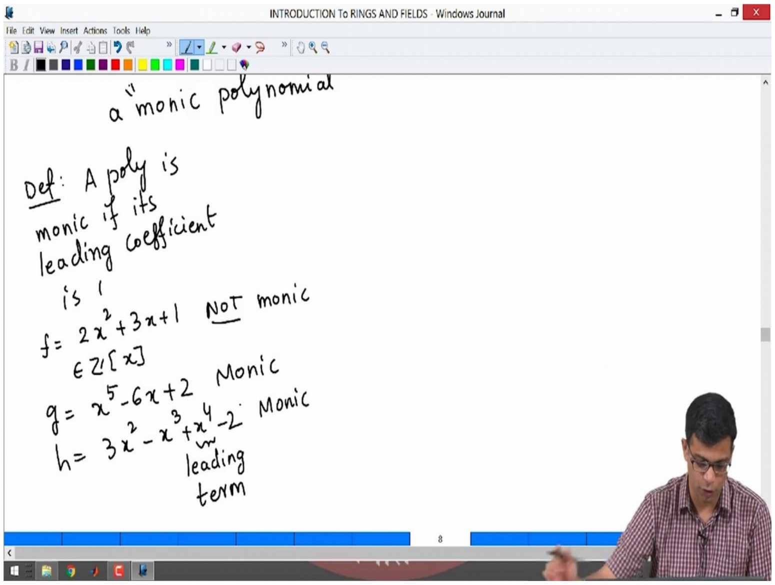
In $R[x]$, we can <u>sometimes</u> divide polynomials.

Given two polynomials $f, g \in R[x]$ with $f(x)$

a "monic polynomial"

So, in R[x] we can sometimes I will write, not always, divide polynomials; so, what is it that I want do ok. So, I am going to quickly do this I will not write the formal procedure, I will just explain the procedure by an example, this is the usual division of numbers it is a same procedure that you all know for very well. So, the statement is given; so R and f are R is arbitrary ring R[x] is a polynomial ring over it. So, given two polynomials f and g in R x with f let us say monic polynomial. So, I do not know if I defined this. So, what is a monic polynomial?

(Refer Slide Time: 23:34)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
8

a "monic polynomial"

Def: A poly is monic if its leading coefficient is 1

$f = 2x^2+3x+1$ NOT monic $\in \mathbb{Z}[x]$

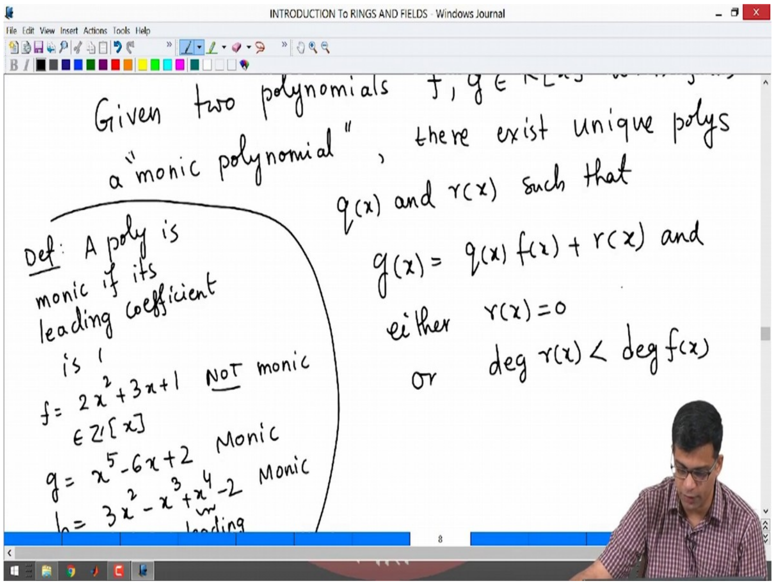
$g = x^5-6x+2$ Monic

$h = 3x^2 - x^3 + \underbrace{x^4}_{\text{leading term}} - 2$ Monic

So, I will quickly define what is a monic polynomial and then I will continue this. Definition: a polynomial is monic if its leading coefficient is 1 ok. So, what is the leading coefficient? It is the coefficient with the largest degree. So, for example, f equals 2 x squared plus 3 x plus 1 is not let us say inside Z[x], it is not monic right, its leading coefficient is 2.

On the other hand g is x power 5 minus 6 x plus 2 is monic and what about h; h is 3 x squared minus x cube plus x 4 minus 2 is also monic right, because even though I have not written them in the correct order the leading term is this; leading term is by definition the term with the largest degree. So, here the leading term is x power 4 and its coefficient is 1. So, it is monic ok, so this is a side definition.

(Refer Slide Time: 25:07)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
8

Given two polynomials $f, g \in$

a "monic polynomial", there exist unique polys $q(x)$ and $r(x)$ such that

$g(x) = q(x) f(x) + r(x)$ and

either $r(x) = 0$

or $\deg r(x) < \deg f(x)$

Def: A poly is monic if its leading coefficient is 1

$f = 2x^2 + 3x + 1$ NOT monic $\in \mathbb{Z}[x]$

$g = x^5 - 6x + 2$ Monic

$h = 3x^2 - x^3 + \underbrace{x^4}_{} - 2$ Monic

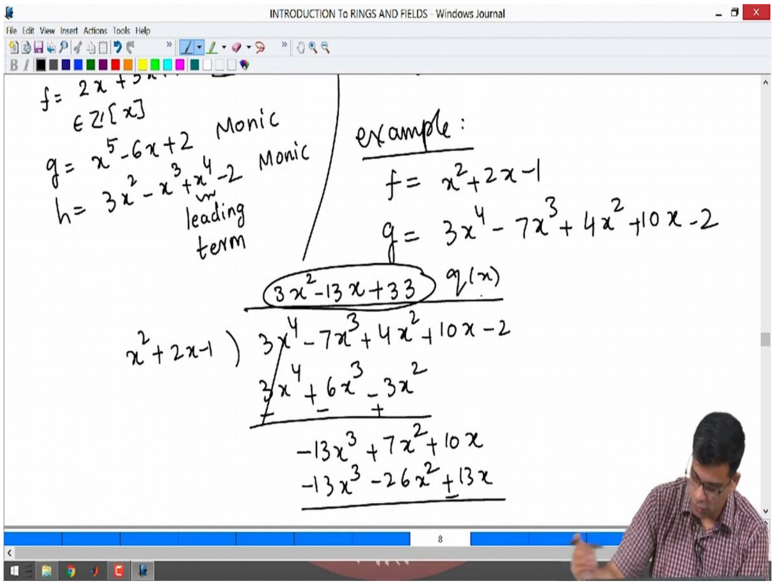
leading

Now, let us come back here given two polymers f and g with f(x) a monic polynomial we can divide g by f; what is a division really mean? It means the following, there exist unique polynomials q(x) and r(x) such that we can write g(x) as q(x) times f(x) plus r(x) and the r(x); obviously, stands for the reminder for this division. We have two possibilities either r(x) is 0 or r(x) can be 0 or we can define the degree of r(x) if it is not the 0 polynomial.

Remember, degree is the largest degree that appears in the polynomial must be strictly less than degree of f(x). So, I suggest that you think about this carefully this is exactly what we mean by division for integers. For example, if you have two integers we can divide one by the other and we can; that means, we can write it like this there the reminder is always strictly less than it is a non-negative number. So, either 0 or its positive, if it is positive it is strictly less than what you have divided with ok. So, that's all; we can always do this.

So, in order to explain I mean, you can prove this, but that will take me I mean that is unnecessary to do this you are all familiar with this. So, to explain what really happens I will simply just do an example ok. So, quickly let me do this.

(Refer Slide Time: 26:52)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help

$f = 2x + 3x$

$\in \mathbb{Z}[x]$

$g = x^5 - 6x + 2$ Monic

$h = 3x^2 - x^3 + \underbrace{x^4}_{\text{leading term}} - 2$ Monic

example:

$f = x^2 + 2x - 1$

$g = 3x^4 - 7x^3 + 4x^2 + 10x - 2$

$$\boxed{3x^2 - 13x + 33} \quad q(x)$$

$$x^2+2x-1 \;)\; 3x^4 - 7x^3 + 4x^2 + 10x - 2$$

$$\cancel{3x^4} + 6x^3 - 3x^2$$

$$-13x^3 + 7x^2 + 10x$$

$$-13x^3 - 26x^2 + 13x$$

So, what we will do is we will take f to be, so I have written this here x square plus 2 x minus 1 and g to be 3 x 4 minus 7 x cubed plus 4 x squared minus 10 x or plus 10 x minus 2 ok. So, let me just do an example. So, here I want to divide this, this is the usual Euclidean division algorithm.

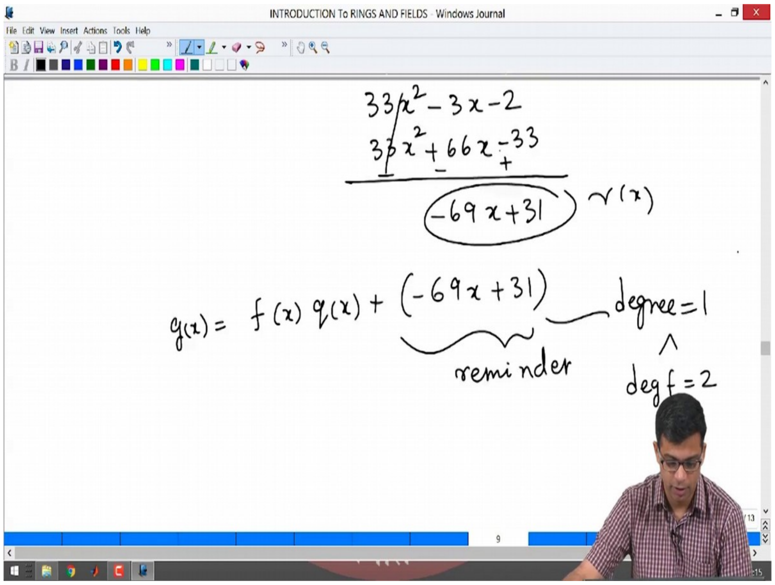
So, we have x squared plus 2 x minus 1 here 3 x 4 minus 7 x cubed plus 4 x squared plus 10 x minus 2. So, I am going to write the terms here. So, first I want to divide 3 x 4 by x squared, how do you do that? That is simply 3 x squared. Here you see why I need the leading term to be 1 because if it is not 1 I may not be able to get 3 that I want. So, I will describe this again in examples.

So, x squared times 3 x squared is 3 x 4; you have plus 6 x cubed minus 3 x squared. So, now, you subtract right, so in other words you change signs; so you cancel this. So, what you have is minus x cubed. So, let us see yeah sorry, this is actually plus becomes minus so, minus 7 minus 6 is minus 13 x cubed, then you have 7 x squared and you can also bring down 10 x.

So, next you want to cancel minus 13 x cubed, so you get minus 13 x here right. So, minus 13 x, so that is minus 13 x cubed minus 26 x squared plus 13 x. So, now you subtract again what you get it is 33 x squared, so you subtract minus 3 x is what you get and you have a minus 2 from before. So, you write minus 2.

Now, you want to cancel 33 x squared. So, what you get is 33 just 33; so, you get 33 x squared plus 66 x right 33 x squared, 33 times 2 x is 66 x minus 33 ok. So, then you subtract again, so this minus minus plus. So, this will cancel what you have is minus 69 x and plus 31; so that is all. So, this will be q now this will be r and this will be q(x).

(Refer Slide Time: 30:02)


INTRODUCTION To RINGS AND FIELDS - Windows Journal
File Edit View Insert Actions Tools Help
9
13

$$\cancel{33x^2} - 3x - 2$$

$$\underset{-}{\cancel{33x^2}} \underset{-}{+} 66x \underset{+}{-} 33$$

$$\boxed{-69x + 31} \quad r(x)$$

$$g(x) = f(x)\, q(x) + \underbrace{(-69x + 31)}_{\text{reminder}} \quad \text{degree} = 1$$

$$\wedge$$

$$\deg f = 2$$

So, we have written the polynomial f g as f(x) times, so g(x) I will write, g(x) as f(x) times q(x) I am mainly interested in the reminder. So, reminder is minus 69 x plus 31 ok. So, this is the reminder and remember what is the property of the reminder it is either 0 in this case it is not 0 or its degree strictly less than degree of f.

What is the degree of the reminder? It is 1 which is strictly less than degree of f which is 2. This is not surprising right because we can always continue the division procedure until the reminder is of smaller degree because if it is bigger degree or if it is at least degree equal to degree of the polynomial you are dividing by you can continue. So, you will go until you have a reminder of small degree or you get 0.

So, I hope this is clear the procedure is just very simple. So, we can always divide one polynomial by another monic polynomial. So, I will stop this video here and in the next video we will discuss a little bit more about division inside a polynomial ring and we will study a few more properties of the polynomial ring

Thank you.